UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/828,695	04/05/2001	Ernie F. Brickell	10559/458001/P10869	6460

20985　　7590　　10/05/2004		

FISH & RICHARDSON, PC
12390 EL CAMINO REAL
SAN DIEGO, CA 92130-2081

EXAMINER
NORRIS, TREMAYNE M

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/828,695	BRICKELL, ERNIE F.
	Examiner	**Art Unit**	
	Tremayne M. Norris	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>05 April 2001</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-30</u> is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-30</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>05 April 2001</u> is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All   b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Drawings

1.   The drawings are objected to under 37 CFR 1.83(a). The drawings must show

every feature of the invention specified in the claims. Therefore, the limitation of

receiving secured information from a source that is other than the client and is "other

than the server" as stated in claim 20 must be shown or the feature(s) canceled from

the claim(s). No new matter should be entered.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in

reply to the Office action to avoid abandonment of the application. Any amended

replacement drawing sheet should include all of the figures appearing on the immediate

prior version of the sheet, even if only one figure is being amended. The figure or figure

number of an amended drawing should not be labeled as "amended." If a drawing figure

is to be canceled, the appropriate figure must be removed from the replacement sheet,

and where necessary, the remaining figures must be renumbered and appropriate

changes made to the brief description of the several views of the drawings for

consistency. Additional replacement sheets may be necessary to show the renumbering

of the remaining figures. The replacement sheet(s) should be labeled "Replacement

Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of

the drawing figures. If the changes are not accepted by the examiner, the applicant will

be notified and informed of any required corrective action in the next Office action. The

objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

2.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3.   Claims 1-4,6-8,10,11,16-20,23-26,29,30 are rejected under 35 U.S.C. 102(b) as

being anticipated by Gennaro et al (US pat 5,937,066).

Regarding claim 1, Gennaro teaches a method comprising:

defining a key and a set of values, the key being determined by the values

and a predefined relationship,

sending one of the values the set and information encrypted using the key

server; and

sending another of the values of the set to a first delegate (col.5 line 65

thru col.6 line 39; col.9 lines 5-38).

Regarding claim 2, Gennaro teaches generating second set of values, the key

being also determined by the values of the second set;

sending one of the values of the second set to the server (col.9 lines 16-17); and

sending another of the values of the second set second delegate (col.13 lines 8-12).

Regarding claim 3, Gennaro teaches the values of the second set are also determined by the predefined relationship (col.5 line 65 thru col.6 line 39; col.9 lines 5-38).

Regarding claim 4, Gennaro teaches the set includes exactly two values (col.9 lines 8-13).

Regarding claim 6, Gennaro teaches the value of the set sent to the server is associated with a descriptor of the first delegate (col.15 lines 58-67; col.17 lines 30-38).

Regarding claim 7, Gennaro teaches the probability of guessing the key correctly using knowledge of one or more of the values of the set, but not all the values of the set is the same as the probability of guessing the key correctly using no knowledge of any value of the set (col.6 lines 35-39).

Regarding claim 8, Gennaro teaches the predefined relationship comprises the Boolean XOR function or a relationship that applies an encryption algorithm to one

value of the set using another value of the set as the encryption algorithm key (col.18 lines 51-67).

Regarding claim 10, Gennaro teaches a method comprising:

storing, on a server accessible through a network, secured information and a first access component, use of the secured information requiring the first access component and a second access component (col.5 line 65 thru col.6 line 39; col.9 lines 5-38); and

providing the secured information and the first access component to a first requestor (col.9 lines 20-24).

Regarding claim 11, Gennaro teaches the second access component is not stored on the server (col.17 lines 25-48; access components go directly to delegates).

Regarding claim 16, Gennaro teaches storing permission information about the identity of a party approved for access, such that the secured information and the first access component are only provided if the first requestor is an approved party (col.15 lines 58-67; col.17 lines 30-38)

Regarding claim 17, Gennaro teaches the secured information is secured by encryption using a key, and the first and second access components are related to the key by a predefined relationship (col.5 line 65 thru col.6 line 39; col.9 lines 5-38).

Regarding claim 18, Gennaro teaches a method comprising:

receiving

a) from a client, a first access component required for use of secure information, the use requiring the first access component and a second access component,

b) from a server accessible through a network, the secured information, and

c) from a source other than the client, the second access component (col.5 line 65 thru col.6 line 39; col.9 lines 5-38).

Regarding claim 19, Gennaro teaches the source is the server (col.9 lines 20-24).

Regarding claim 20, Gennaro teaches the source is other than the server (col.17 lines 25-48; access components go directly to delegates).

Regarding claim 22, Gennaro teaches the secured information, the first access component, and the second access component are received in a digital form (col.13 lines 3-5).

Claims 23 and 24 are substantially equivalent to claims 1 and 2 respectively,

therefore claims 23 and 24 are rejected because of similar rationale.

Regarding claim 25, Gennaro teaches an apparatus comprising a processor and

instructions configured to cause the processor to:

receive, from a client, information and a value of a set values, the information

being encrypted using key, the key being determined by the values of the set and a

predefined relationship;

store the information and the value, but not all the values of the set; and

transmit, a delegate, the information and the value (col.5 line 65 thru col.6 line

39; col.9 lines 5-38).

Regarding claim 26, Gennaro teaches store a second value that is a member of

a second set of values, the values of the second set being sufficient to determine the

key using the predefined relationship (col.5 line 65 thru col.6 line 39; col.9 lines 5-38).

Regarding claim 29, Gennaro teaches a method comprising:

encrypting information using an encryption key;

sending the encryption key, but not the encrypted information to a first

party;

sending the encrypted information, but not the encryption key to a server

(col.5 line 65 thru col.6 line 39; col.9 lines 5-38).

Claim 30 is substantially equivalent to claim 6, therefore claim 30 is rejected

because of similar rationale.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 5,12-15,21,27 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Gennaro, and further in view of Price (US pat 6,662,299).

Regarding claim 5, Gennaro teaches the method of claim 1, but does not teach

the set includes three or more values. Price teaches the set includes three or more

values (col.2 lines 1-25). It would have been obvious to one of ordinary skill in the art at

the time of the invention to combine Gennaro's cryptographic key recovery system with

Price's method for reconstituting an encryption key in order to provide a system that

allows encryption keys to be reconstructed without requiring a user to remember a

specific password (Price col.1 lines 65-67).

Regarding claim 12, Gennaro teaches the method of claim 10, but does not

teach storing a third access component, such that the third access component and a

fourth access component are sufficient to permit use of the secured information. Price

teaches storing a third access component, such that the third access component and a

fourth access component are sufficient to permit use of the secured information (col.3

lines 3-5; col.5 lines 7-37). It would have been obvious to one of ordinary skill in the art

at the time of the invention to combine Gennaro's cryptographic key recovery system

with Price's method for reconstituting an encryption key in order to provide a system

that allows encryption keys to be reconstructed without requiring a user to remember a

specific password (Price col.1 lines 65-67).

Regarding claim 13, Gennaro and Price in combination teach the method of

claim 12, in addition Gennaro teaches providing the secured information and the third

access component to a second requestor (col.13 lines 8-12).

Regarding claim 14, Gennaro and Price in combination teach the method of

claim 12, in addition Price teaches deleting the third access component in response to a

trigger, trigger being a client instruction, a time limit, request from the first requestor, a

security breach (col.7 line 58).

Regarding claim 15, Gennaro and Price in combination teach the method of

claim 12, in addition Price teaches identifying the requestor and determining that the

requestor requires the first access component but not the third access component (col.5 lines 7-37).

Regarding claim 21, Gennaro teaches the method of claim 18. What Price teaches that Gennaro does not teach is a third access component is required in addition to the first and second access components for use of the secured information (col.5 lines 7-37). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Gennaro's cryptographic key recovery system with Price's method for reconstituting an encryption key in order to provide a system that allows encryption keys to be reconstructed without requiring a user to remember a specific password (Price col.1 lines 65-67).

Claim 27 is substantially equivalent to claim 14, therefore claim 27 is rejected because of similar rationale.

6.   Claims 9 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro.

Regarding claim 9 and 28, examiner takes official notice that the protection of medical information is well known in the security art. It would have been obvious to one of ordinary skill in the art at the time of the invention to try to keep medical information secure because medical information is one of numerous types of information that is

known to be private to those who the information is about, and encryption would have

been an obvious method in order to keep that information private only to those

authorized to view it.

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Tremayne M. Norris whose telephone number is (571)

272-3874. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate

Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone

number for the organization where this application or proceeding is assigned is 703-

872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Tremayne Norris

September 29, 2004